Date: Thu, 14 Apr 94 04:30:26 PDT
From: Ham-Digital Mailing List and Newsgroup <ham-digital@ucsd.edu>
Errors-To: Ham-Digital-Errors@UCSD.Edu
Reply-To: Ham-Digital@UCSD.Edu
Precedence: Bulk
Subject: Ham-Digital Digest V94 #113
To: Ham-Digital

Ham-Digital Digest Thu, 14 Apr 94 Volume 94 : Issue 113

Today's Topics:

Send Replies or notes for publication to: <Ham-Digital@UCSD.Edu>
Send subscription requests to: <Ham-Digital-REQUEST@UCSD.Edu>
Problems you can't solve otherwise to brian@ucsd.edu.

Archives of past issues of the Ham-Digital Digest are available
(by FTP only) from UCSD.Edu in directory "mailarchives/ham-digital".

Date: 13 Apr 94 18:35:55 GMT
From: spsgate!mogate!newsgate!news@uunet.uu.net
Subject: 486cpu RFI Problems
To: ham-digital@ucsd.edu

I have been trying to set up a packet station, and have
experienced problems due to a LOT of noise emitted by my
PC. I thought those devices were supposed to be relatively
shielded, but even with an external antenna, my HT pickes
up a lot of noise, which makes squelch settings, etc.
difficult.

Does anyone know of a way to quiet the environment down
to make it more acceptable to Ham. I have tried different
ac outlets but it makes no difference.

Thanks

rick

--
R i c k C o t t l e
Email:rrbk50@email.sps.mot.com

Date: 13 Apr 1994 05:17:31 GMT
From: ihnp4.ucsd.edu!library.ucla.edu!europa.eng.gtefsd.com!
howland.reston.ans.net!wupost!crcnis1.unl.edu!unlinfo.unl.edu!
mcduffie@network.ucsd.edu
Subject: FCC Packet Message Forwarding
To: ham-digital@ucsd.edu

brian@nothing.ucsd.edu (Brian Kantor) writes:

>Remember the primitive level of most ham stations.

This reminds me... Someone, a few posts back, made the comment that most packet bbs stations now sport at least a 486 computer with several hundred megabytes of hard drive. I would like to dispute that comment. Yes, there are some systems like that. And, the number is on the increase. But, I doubt that even half of them are. Remember, there are many people still getting along quite well on an XT class machine.

Until last weekend, my XT with 40m HD was my main board, running FBB, SAM, BPQ, and several ports. I was finally able to upgrade my "office" computer to a 386 and took the 286 back to the shack to replace the XT. The 286 is more than enough computer to handle the job and is quite fast. I would hate to see the day that we had to have other than a minimal computer to handle bbs software.

73 - Gary

Date: Wed, 13 Apr 94 01:46:05 GMT
From: ihnp4.ucsd.edu!mvb.saic.com!news.cerf.net!usc!howland.reston.ans.net!agate!
library.ucla.edu!csulb.edu!csus.edu!netcom.com!netcomsv!skyld!
jangus@network.ucsd.edu
Subject: FCC Packet Message Forwarding
To: ham-digital@ucsd.edu

In article <WAF.94Apr12153047@sunfish.zk3.dec.com> waf@sunfish.zk3.dec.com writes:

> (Note that even if you use the original RSA signature scheme
> of encrypting the entire message with your private key, the purpose
> isn't to obscure the content, so you are probably safe. Since it can
> be decrypted with your public key, you should be really safe. Even
> more if you append your public key to the message.)

It is my understanding that the encryption only has to be the "signature" not the body of the message. No sense in getting the "I can't copy on my Model 15 types more upset about things than normal.

Amateur: WA6FWI@WA6FWI.#SOCA.CA.USA.NOAM | "You have a flair for adding
Internet: jangus@skyld.grendel.com | a fanciful dimension to any
US Mail: PO Box 4425 Carson, CA 90749 | story."
Phone: 1 (310) 324-6080 | Peking Noodle Co.

Date: 13 Apr 1994 17:17:55 GMT
From: news.mentorg.com!hpbab33.mentorg.com!wv.mentorg.com!hanko@uunet.uu.net
Subject: FCC Packet Message Forwarding
To: ham-digital@ucsd.edu

In article <2od03d$hpe@network.ucsd.edu>, brian@nothing.ucsd.edu (Brian Kantor) writes:
|> Doug Rickard writes:
|> >A good system for 'client' authentication already exists in the form of
|> >Kerberos from MIT. Perhaps we should see if a variant of Kerberos is
|> >appropriate for PBBS user authentication. After all, why re-invent the wheel.
|>
|> Current ham radio networks lack the bandwidth, and most ham stations
|> lack the computing power to do Kerberos.
|>
|> I suspect you'll find that most of the cryptographic signature and/or
|> authentication systems can't be run inside a TNC.
|>
|> Remember the primitive level of most ham stations. You'll probably have
|> to use some one-time-pad or equivalent paper-based authenticator scheme
|> if Joe Ham is going to use your system.
|>
|> Sorry.
|> - Brian

I suspect most BBS systems run on minimum 386 today, and many, at least one per major area, run a fast 486 or even P5.

So the authentication using various schemes is certainly possible.

Note that what is actually required is to verify that the station
connected to the BBS is actually who they say they are: i.e. that
the connect to the BBS was done by the holder of the callsign.

There are many schemes that can provide this verification at high
level of certainty, without requiring any more processing than
a Z-80 can provide.

Providing authentication for the contents of a message is a different
issue. Do we need to address this also? My reading of the rules says we
do not.

   ... Hank

--

Hank Oredson @ Mentor Graphics
Internet   : hank_oredson@mentorg.com
Amateur Radio: W0RLI@W0RLI.OR.USA.NOAM

Date: 12 Apr 94 12:05:57 EDT
From: agate!howland.reston.ans.net!europa.eng.gtefsd.com!darwin.sura.net!wvnvms!
marshall.wvnet.edu!desaid@ames.arpa
Subject: help with NTS address.. newbie..:)
To: ham-digital@ucsd.edu

HI all:

I just setting up a packet TNC and I was wondering how do I get NTS address
and AMPR address for my call sign.

Any help will be appreicated. I live in Huntington, WV and my call sign is
KB8PHZ.

Thanks a lot.

73
Dinakar
kb8phz

Date: Wed, 13 Apr 94 04:30:23 GMT
From: news.mtholyoke.edu!nic.umass.edu!usenet@uunet.uu.net
Subject: Is KA9Q telnet correct? (virtual terminal)
To: ham-digital@ucsd.edu

About a week ago I posted a query re:

Is KA9Q NOS Telnet virtual terminal definition correct?

Thank you to a number of people who wrote me directly or posted followups to my query.

Unfortunately I was unable to keep up with news this week and I found that two followups, from hammock and dave, were still listed in my news server database but expired before I had a chance to read them. Would these people be kind enough to mail me their comments?

As to the problem of KA9Q NOS behavior, at this point I am convinced that the end-of-line handling problem is in the telnet server part of the Minix TCP/IP implementation and not in NOS. Another user has offered me a patch that I hope will resolve the problem.

In a separate post I asked about some other problems I had with NOS dropping the first character on a line and having trouble handling large amounts of quickly-arriving data from a large host. I haven't received any replies on these queries and I would like again to ask for help on understanding and possibly dealing with these problems.

Albert S. Woodhull
Hampshire College, Amherst, MA, USA
awoodhull@hamp.hampshire.edu

Date: 14 Apr 94 00:47:30 GMT
From: sdd.hp.com!vixen.cso.uiuc.edu!prairienet.org!k9cw@hplabs.hp.com
Subject: Look for info on TINY-2 or TNC-2 '4' a friend.
To: ham-digital@ucsd.edu

In a previous article, da884@cleveland.Freenet.Edu (David Toste) says:

>... Ideally, I would like source for a TINY-2, but
>a copy fo the code for real TAPR-2s would be OK. Any other TNC would
>...

Hey - there is an easy solution. Just call up PacComm and ask them for the source listing. I'm certain they will provide an appropriate response. I know I would...

73, Drew

--
------------------------------------------------------------------*
| Andrew B. White K9CW | internet: k9cw@prairienet.org |
| ABW Associates, Ltd. | phone/fax: 217-643-7327 |
------------------------------------------------------------------*

Date: Wed, 13 Apr 1994 03:22:37 GMT
From: gsm001!gsm001.mendelson.com!gsmlrn@uunet.uu.net
Subject: Software for MFJ C64 TNC
To: ham-digital@ucsd.edu

Pardon me for being vague, but I was talking to a ham who purchased an MFJ TNC that plugs into his Commodore 64. It is supposed to use "public domain" software. It did not come with any software :-(

I don't think this is a regular TNC with an rs232 to ttl converter, but a small circuit card with an edge connector unique to the C64. Based on the price I expect that it is only a modem. The packet assembly/disasembly/AX.25 processing is done in the C64.

He does not have access to the Internet nor packet.

I have looked in both the C64 archives at U. Waterloo and at the ham radio archives at oak.oakland.edu. I could not find anything appropriate.

Does anyone know what software to use? If you do where do I get it? (file names too please) Once I get it how, do I get it onto a C64 Disk?

Thanks for your time and trouble.

73,

Geoff.

--
"I am number six. Others come and others go, but I am always number six."
(From the movie "Eminent Domain".)

Geoffrey S. Mendelson N3OWJ   (215) 242-8712 gsm@mendelson.com

---

Date: Wed, 13 Apr 1994 19:12:44 GMT
From: ihnp4.ucsd.edu!news.cerf.net!pravda.sdsc.edu!nic-nac.CSU.net!
charnel.net.csuchico.edu!charnel!olivea!sgigate.sgi.com!sgiblab!pacbell.com!att-
out!cbnewsj!kb2glo@network.ucsd.edu
Subject: TCP/IP NOS FAQ?
To: ham-digital@ucsd.edu

I'm interested in getting NOS on the air however there seem to be so many
different versions! Does anybody have a FAQ regarding all the different
versions of NOS so I can make an intelligent decision on which one to use.

Thanks and 73, Tom Kenny KB2GLO

--
Tom Kenny, KB2GLO
UUCP: ...!att!lzusp!tek Internet: tek@lzusp.att.com
Packet Radio: KB2GLO@WT3V.NJ.USA Voice Telephone: 908-576-3888

Date: Wed, 13 Apr 1994 14:01:04 GMT
From: agate!howland.reston.ans.net!europa.eng.gtefsd.com!news.umbc.edu!eff!
news.kei.com!yeshua.marcam.com!zip.eecs.umich.edu!newsxfer.itd.umich.edu!
news1.oakland.edu!rcsuna.gmr@ihnp4.ucsd.edu
To: ham-digital@ucsd.edu

References <JAY.19.2DA5AFB8@medicine.dmed.iupui.edu>,
<2oaalr$hm3@search01.news.aol.com>, <WAF.94Apr12153047@sunfish.zk3.dec.com>sh
Reply-To : anderson@kosepc01.delcoelect.com (Alan Anderson)
Subject : Re: FCC Packet Message Forwarding

In <WAF.94Apr12153047@sunfish.zk3.dec.com>, waf@sunfish.zk3.dec.com (William
Freeman USG) writes:
>.... Since it can
>be decrypted with your public key, you should be really safe. Even
>more if you append your public key to the message.)

Oops! If you use the public key in the message to authenticate the message,
you can be fooled easily. You will know that the message was signed by the
private key corresponding to that public key. You won't know that the keys
belong to anybody in particular.

In order for digital signatures to work, the public keys must be distributed
by a trusted mechanism (which is NOT a chicken-and-egg problem, BTW -- there
are several schemes to "bootstrap" the trust).

========
Alan Anderson (WB9RUF) [no fancy .sig -- yet]

Date: 13 Apr 94 15:05:57 GMT
From: sdd.hp.com!col.hp.com!jms@hplabs.hp.com
To: ham-digital@ucsd.edu

References <2nph5e$djt@hpbab.mentorg.com>, <2obmb7$bme@hp-col.col.hp.com>,
<2oer1m$rp3@hpbab.mentorg.com>
Subject : Re: NTS traffic on packet

: " ... out of a total of 8 messages ..."

: You mean only eight messages arrived at the BBS during that day?
: Amazing ...

That's the ones that were auto-forwarded to me by just one bbs here in
the Colorado Springs area.

Mike, K0TER

Date: 14 Apr 94 00:17:52 GMT
From: juniper.almaden.ibm.com!enge.almaden.ibm.com!enge@uunet.uu.net
To: ham-digital@ucsd.edu

References <JAY.24.2DA96766@medicine.dmed.iupui.edu>,
<2od0cl$hqk@network.ucsd.edu>, <2oha1j$3qp@hpbab.mentorg.com>com
Subject : Re: FCC Packet Message Forwarding

The authentication scheme in use by my code is MD5.

Roy Engehausen, AA4RE
enge@almaden.ibm.com

Date: 13 Apr 1994 17:27:15 GMT
From: news.mentorg.com!hpbab33.mentorg.com!wv.mentorg.com!hanko@uunet.uu.net
To: ham-digital@ucsd.edu

References <2oaalr$hm3@search01.news.aol.com>,
<JAY.24.2DA96766@medicine.dmed.iupui.edu>, <2od0cl$hqk@network.ucsd.edu>≥„
Reply-To : Hank_Oredson@mentorg.com

Subject : Re: FCC Packet Message Forwarding

In article <2od0cl$hqk@network.ucsd.edu>, brian@nothing.ucsd.edu (Brian Kantor)
writes:
|> JAY@medicine.dmed.iupui.edu (Jay Sissom) writes:
|> >RSA & PGP would be OK, except they might be interpreted as illegal encryption.
|>
|> If you just want to make sure the message isn't forged, sign an MD5
|> checksum of the message with your RSA private key. Since no information
|> is hidden in such, it's clear that it isn't an illegal encryption.
|>
|> If the MD5 checksum matches, the message is unaltered. If you were able
|> to decrypt the MD5 checksum in the first place, you're authenticated the
|> sender.
|>
|> [Above scheme stolen from the MUSE project.]
|>
|> Export and international issues are your problem to solve.
|>   - Brian

And if you want to do this with less processing time, use MD4 or even MD2.
Brain, ka2bqe, has an MD5 implementation running with compressed batch
forwarding, not for verification purposes, but to allow better error
detection.

In the longer run, the ham digital network is certainly moving toward the
use of these existing standards. The use of RSA plus MD5 makes a lot of
sense.

   ... Hank

--

Hank Oredson @ Mentor Graphics
Internet   : hank_oredson@mentorg.com
Amateur Radio: W0RLI@W0RLI.OR.USA.NOAM

Date: 13 Apr 94 15:06:57 GMT
From: sdd.hp.com!col.hp.com!jms@hplabs.hp.com
To: ham-digital@ucsd.edu

References <2nf770$l66@hpbab.mentorg.com>, <2oblv6$bme@hp-col.col.hp.com>,
<2oer3v$rp3@hpbab.mentorg.com>
Subject : Re: NTS traffic on packet

Hank Oredson (hanko@wv.mentorg.com) wrote:

: In article <2oblv6$bme@hp-col.col.hp.com>, jms@col.hp.com (Mike Stansberry)
writes:
: |> Hank Oredson (hanko@wv.mentorg.com) wrote:
: |> : In article <CnFLr1.Hu8@cbnewsh.cb.att.com>, ostroy@cbnewsh.cb.att.com (Dan
Ostroy) writes:
: |>
: |> : The days of handling traffic on 80M CW are pretty much gone now, just
: |>   ^^^^^^
: |> **** WRONG!!! *** Just because YOU don't do it, don't assume it's
: |> gone. I handle a LOT of traffic on 80M (and 40M) CW and so do a
: |> lot of others!
: |>
: |> Mike, K0TER
: |>

: I'm certainly sorry to hear that.

: Sounds terribly inefficient and error prone, when there are
: better ways to do it.

: --

: Hank Oredson @ Mentor Graphics
: Internet   : hank_oredson@mentorg.com
: Amateur Radio: W0RLI@W0RLI.OR.USA.NOAM

I guess you are just not interested in trying to help. Use your
system or none at all, right? End of discussion.

Mike, K0TER

End of Ham-Digital Digest V94 #113
****